UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff*, v. DMITRY STAROVIKOV; ALEXANDER FILIPPOV; Does 1-15, *Defendants*.	Civil Action No. 1:21-cv-10260-DLC

[PROPOSED] FINAL DEFAULT JUDGMENT
AND ORDER FOR PERMANENT INJUNCTION

Defendants Dmitry Starovikov and Alexander Filippov ("Defendants") have filed a Motion to Vacate Entry of Default and to Dismiss This Action. Plaintiff Google LLC has filed a motion for Default Judgment and a Permanent Injunction to enjoin Defendants Dmitry Starovikov and Alexander Filippov, and Does 1 through 15—through their participation in, and operation of, the Glupteba Enterprise—from continuing to control and operate a botnet of over a million devices, continuing to distribute malware to infect new devices, and continuing to carry out criminal schemes.

Google filed a complaint alleging claims under: (1) the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1962(c)–(d) (Count I); (2) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (Count II); (3) the Electronic Communications Privacy Act, 18 U.S.C. § 2701 (Count III); (4) the Lanham Act (Count IV); (5) and

common-law theories of tortious interference with business relationships and unjust enrichment (Counts V–VI).

THE COURT HEREBY FINDS THAT:

Jurisdiction and Venue

1. This Court has federal-question jurisdiction over Google's claims under the Racketeer Influenced and Corrupt Organizations Act, the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and the Lanham Act under 28 U.S.C. § 1331. This Court also has jurisdiction over the Lanham Act and related state and common law unfair competition claims under 28 U.S.C. § 1338 and 15 U.S.C. § 1121, respectively. This court has supplemental jurisdiction over the state-law claims under 28 U.S.C. § 1367.

2. This Court has personal jurisdiction over the Defendants because:

   a. Defendants waived any objection to personal jurisdiction by representing to the Court and to Google that they would consent to personal jurisdiction;

   b. The Defendants distribute malware to Google users in this district and within the state of New York;

   c. The Defendants send commands to infected user computers in this district and within New York to carry out illicit schemes; and

d. Google's complaint and moving papers demonstrate that the Defendants undertook these activities intentionally with knowledge that their actions would cause harm to users in New York, and cause Google harm in New York. Google does business in New York and has done business in New York for many years.

3. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are not residents of the United States and may be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C. § 1391(b) and 18 U.S.C. § 1965 because: a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district; a substantial part of the property that is the subject of Google's claims is situated in this judicial district; a substantial part of the harm caused by Defendants has occurred in this judicial district; and Defendants transact their affairs in this judicial district. Moreover, Defendants are subject to personal jurisdiction in this district and no other venue appears to be more appropriate.

4. The complaint pleads facts with the specificity required by the Federal Rules and states claims against Defendants for violations of the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. §§ 1962(c)-(d) (Count I); the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (Count II); the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701 (Count III); the Lanham Act

(Count IV); and common law claims for tortious interference with business relationships and unjust enrichment (Counts V–VI).

Default Judgment

5. Defendants were served by means approved by the Court and failed to timely appear, plead, or otherwise defend against this Action. The requisite time of 21 days between service of the summons and complaint has elapsed. The Clerk properly entered default pursuant to Rule 55(a) on February 8, 2022. ECF No. 38. The evidence indicates that no Defendant is an infant or incompetent.

6. The Court has considered Defendants' Motion to Vacate Entry of Default and to Dismiss This Action, ECF Nos. 47, 47-1, 47-2, 47-3, and Google's Motion for Default Judgment and a Permanent Injunction, ECF No. 48 *et seq*. The Court has further considered the willfulness of Defendants' default, whether Defendants have complete, meritorious defenses to the claims filed against them, and whether setting aside the Certificate of Default would prejudice Google.

7. The Court finds that Defendants have not established good cause to set aside the Certificate of Default and that Google is entitled to Default Judgment against Defendants Starovikov and Filippov and Does 1 through 15.

A Permanent Injunction is Warranted

8. The Court finds that Google has established each of the factors required for a permanent injunction: (1) it has suffered an irreparable injury; (2) remedies available at law are inadequate to compensate for that injury; (3) in light of the

hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) the public interest would not be disserved by a permanent injunction. *World Wide Polymers, Inc. v. Shinkong Synthetic Fibers Corp.*, 694 F.3d 155, 160–161 (2d Cir. 2012) (citing *eBay Inc. v. MercExchange LLC*, 547 U.S. 388, 391 (2006)). The Court also finds that Google has established actual success on the merits of each of its claims. *Amoco Prod. Co. v. Vill. of Gambell, AK*, 480 U.S. 531, 546 n.12 (1987) ("The standard for a preliminary injunction is essentially the same as for a permanent injunction with the exception that the plaintiff must show a likelihood of success on the merits rather than actual success."); *Ognibene v. Parkes*, 671 F.3d 174, 182 (2d Cir. 2011) (quoting *Amoco*).

Irreparable Harm

9. Google has established that it was irreparably injured and that legal remedies are inadequate to compensate for that harm. In particular, it has shown that the Defendants—through their participation in, and operation of, the Glupteba Enterprise—have threatened the security of the internet, including Google platforms, by transmitting malware through the internet to configure, deploy, and operate a botnet. The Enterprise has distributed malware on devices of Google users, compromising the security of those devices and continues to issue commands to those

devices to carry out criminal activities, such as selling access to Google user accounts and selling fraudulent credit cards to use on those accounts.

10. The Defendants control a botnet that has infected more than one million devices. At any moment, the botnet's extraordinary computing power could be harnessed as part of additional criminal schemes. Defendants could, for example, enable large ransomware or distributed denial-of-service attacks on legitimate businesses and other targets. Defendants could themselves perpetrate such a harmful attack, or they could sell access to the botnet to a third-party for that purpose.

11. In addition, Defendants' conduct is infringing Google's trademarks, injuring Google's goodwill, and damaging its reputation by creating confusion as to the source of the Glupteba malware because the Defendants use a domain that infringes Google's YouTube mark to distribute malware. That constitutes irreparable harm.

Adequacy of Remedies at Law

12. The harm done to Google's systems and to its customers would not and cannot be remedied by purely monetary damages, and Google has established that a remedy at law is inadequate for the injuries identified in its moving papers, Complaint, and the accompanying evidence.

Balance of the Hardships

13. The equities also favor a permanent injunction. The criminal enterprise continues to defraud consumers and injure Google. There is no countervailing factor weighing against a permanent injunction as there is no legitimate reason why Defendants should be permitted to continue to disseminate malware and manipulate infected computers to carry out criminal schemes.

Public Interest

14. Google has shown that the public interest favors granting a permanent injunction.

15. Every day that passes, there is substantial risk that Defendants may infect new computers, steal additional account information, and deceive more unsuspecting victims. After receiving notice of the Temporary Restraining Order and Preliminary Injunction, Defendants have continued to engage in conduct enjoined by this Court's Orders. Defendants' criminal enterprise has attempted to establish new command and control ("C2") servers in response to Google's ongoing disruption efforts and have continued to establish new domains in order to reconstitute and support the botnet.

16. Protection from malicious cyberattacks and other cybercrimes is strongly in the public interest, and the public interest is clearly served by enforcing statutes designed to protect the public, such as RICO, the CFAA, the ECPA, and the Lanham Act.

Google Has Established Actual Success On The Merits Of Each Of Its Claims

17. Google has established actual success on the merits as to each of its claims.

18. *CFAA*. Defendants have violated and continue to violate the Computer Fraud and Abuse Act. The CFAA prohibits, among other things, intentionally accessing a protected computer, without authorization, and thereby obtaining information from that computer. *See* 18 U.S.C. § 1030(a)(2)(C). Defendants intentionally accessed thousands of users' computers operating in interstate commerce through the internet, without authorization, to infect them with malware. They did so to obtain information such as account credentials and URL history, which they have then sold to others. This has affected well over ten computers within a one-year span and resulted in damages significantly in excess of $5,000.

19. *ECPA*. Defendants have violated and continue to violate the Electronic Communications Privacy Act. The ECPA prohibits, among other things, "intentionally access[ing] without authorization a facility through which an electronic communication service is provided" to "obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701(a). Defendants have deliberately broken into the accounts of Google users and thereby obtained unauthorized access to emails and other communications stored on Google servers. They did so, and continue do so, with the intent to acquire user credentials and other sensitive content.

20. *Lanham Act*. Defendants violated the Lanham Act because they used Google's YouTube mark—a valid, protectable, registered, and incontestable trademark—in commerce in a manner likely to have caused confusion among consumers by operating a website that used the YouTube mark in the domain name and on the landing page. *See* 15 U.S.C. § 1114(1). In addition, the Lanham Act prohibits "false designations of origin" that are likely to cause confusion as to the "origin, sponsorship, or approval" of a product or service. 15 U.S.C. § 1125(a)(l)(A). It also makes unlawful a false or misleading representation, including a false designation of origin, that "in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of . . . goods, services, or commercial activities." 15 U.S.C. § 1125(a)(l)(B). The Defendants deceived internet users by falsely marketing their malware as software for downloading videos from YouTube, for their own profit, to the detriment of Google and Google's trademarks. By establishing Defendants' liability under the Lanham Act, Google is also entitled to a presumption of irreparable harm. 15 U.S.C. § 1116(a).

21. *RICO*. Defendants have violated and continue to violate the RICO statute.

a. Google has shown that each Defendant was, and still is, an active participant in the operation and management of the Glupteba botnet with direct ties to a C2 server previously associated with proxying activity on infected machines. Defendant Dmitry Starovikov was an administrator of Voltonwork.com. Additionally, the secondary email

address for the Google Workspace Voltronwork.com account was an email containing Defendant Starovikov's name under the Trafspin domain. Defendant Alexander Filippov is another co-conspirator who had email accounts associated with Google Workspace accounts related to Voltronwork.com, Dont.farm, and Undefined.team.

b. Google has established that Defendants formed an enterprise. The Defendants shared a common purpose to spread malware to build a botnet that is deployed for numerous criminal schemes for profit. The Defendants worked together to accomplish this purpose, each playing a role as described above.

c. Google has established that the Defendants engaged in a pattern of racketeering activity. The predicate acts include three separate violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A). Defendants have violated and continue to violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A), resulting in damage as defined in § 1030(c)(4)(A)(i)(VI), by (1) infecting protected computers with malware, (2) transmitting to such protected computers programs designed to carry out their schemes, and (3) transmitting to such protected computers commands to infected computers. For instance, Defendants have intentionally caused damage to "protected computers" by transmitting malware "droppers" to those computers, thereby impairing the integrity of their systems and information, and

allowing Defendants to access those systems. They have also transmitted malware modules to protected computers through the internet. And they have transmitted commands to protected computers through the internet, thereby causing damage to those computers and enabling the Enterprise to utilize these computers in its criminal schemes. Google has shown that the Defendants committed predicate acts, including violations of the federal wire fraud statute, 18 U.S.C. § 1343, federal identity fraud statute, 18 U.S.C. § 1028, and federal access device fraud statute, 18 U.S.C. § 1029.

d. Google has suffered injury to its business or property as a result of Defendants' acts that constitute these predicate offenses.

22. Google has shown that Defendants are liable for New York common law claims of tortious interference with business relationships and unjust enrichment.

FINAL JUDGMENT AND PERMANENT INJUNCTION

IT IS HEREBY ORDERED that Google's Motion for Default Judgment and Entry of a Permanent Injunction is granted and Defendants' Motion to Vacate Entry of Default and to Dismiss This Action is denied.

IT IS FURTHER ORDERED that Defendants are in default, and that judgment is awarded in favor of Google and against Defendants Starovikov and Filippov and Does 1 through 15.

IT IS FURTHER ORDERED that Defendants, any of their officers, agents, servants, employees, attorneys, and all others in active concert or participation with them, who receive actual notice of this Order by personal service or otherwise including by email ("Restrained Parties"), are permanently restrained and enjoined from, anywhere in the world:

1. Intentionally accessing and sending malicious code to Google or the protected computers of Google's customers, without authorization;

2. Sending malicious code to configure, deploy, and/or operate a botnet;

3. Attacking and compromising the security of the computers or networks of Google's users;

4. Stealing and exfiltrating information from computers or computer networks;

5. Creating websites that falsely indicate that such websites are or were associated with Google, YouTube, or any other Google affiliate, including through use of Google's YouTube mark or other false or misleading representations;

6. Configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in Google's pleadings, including but not limited to the C2 servers hosted at, and operating through, the IP Addresses listed in Appendix A to Google's Complaint and through any other component or element of the botnet in any location;

7. Delivering malicious code designed to steal credentials and cookies;

8. Monitoring the activities of Google or Google's customers;

9. Stealing information from Google or Google's customers;

10. Selling access to the accounts of Google's customers;

11. Corrupting applications on victims' computers and networks, thereby using such computers or networks to carry out the foregoing activities;

12. Offering or promoting credit cards to others for use in purchasing services from Google;

13. Misappropriating that which rightfully belongs to Google, Google's customers and users, or that in which Google has a proprietary interest;

14. Using, linking to, transferring, selling, exercising control over, or otherwise owning or accessing domains connected with the Enterprise, its activities, or its use of the botnet;

15. Using, transferring, exercising control over, or accessing any accounts used in the transfer of money or electronic currency, including cryptocurrency, or in the processing of card-based transactions, as a means to further Defendants' unlawful schemes;

16. Undertaking any similar activity that inflicts harm on Google, Google's customers, or the public.

Upon service by mail, email, or text, the Defendants and other Restrained Parties shall be deemed to have actual notice of the issuance and terms of the Default

Judgment and Permanent Injunction Order, and any act by any of the Defendants or the Restrained Parties in violation of any of the terms of the Default Judgment and Permanent Injunction Order may be considered and prosecuted as contempt of Court.

IT IS FURTHER ORDERED that Defendants, their representatives and persons who are in active concert or participation with them are permanently enjoined from:

1. Using and infringing Google's trademarks, including Google's YouTube mark;

2. Using, in connection with Defendants' activities, any products or services with any false or deceptive designation, representations or descriptions of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Google or its customers or users or give Defendants an unfair competitive advantage or result in deception of consumers; and

3. Acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Google, or otherwise passing off Defendants' activities, products or services as Google's.

IT IS FURTHER ORDERED that Google may serve this Order on the persons and entities providing services, including domain name registrars, name servers, web hosting services, and other internet service providers, relating to the domains and IP addresses identified by Google as connected to the Enterprise, its

activities, or its botnet, requesting that those persons and entities take reasonable best efforts to implement the following actions:

1. Take reasonable steps to identify incoming and/or outgoing internet traffic on their respective networks that originates and/or is being sent from and/or to such identified domains and IP addresses.

2. Take reasonable steps to block incoming and/or outgoing internet traffic on their respective networks that originate and/or are being sent from and/or to such identified domains and IP addresses except as explicitly provided for in this Order.

3. Take other reasonable steps to block such traffic to and/or from any other IP addresses or domains to which Defendants or Defendants' representatives moved the botnet infrastructure, to ensure that Defendants cannot use such infrastructure to control the botnet;

4. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with such identified domains and IP addresses and make them inaccessible from any other computer on the internet, any internal network, or in any other manner, to Defendants, Defendants' representatives, and all other persons, except as otherwise ordered herein;

5. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with such identified domains and IP addresses;

6. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives until the steps required by this Order are executed in full, except as necessary to communicate with hosting companies, data centers, Google, or other ISPs to execute this Order;

7. Not enable, and take all reasonable steps to prevent, any circumvention of this Order by Defendants or Defendants' representatives associated with such identified domains and IP addresses, including, without limitation, not enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain other domains and IP addresses;

8. Preserve, retain, and produce to Google all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling such identified domains and IP addresses, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers, telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with the use of or access to such domains and IP addresses;

9. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order; and

10. Completely preserve the computers, servers, electronic data storage devices, software, data, or media assigned to or otherwise associated with such

identified domains and IP addresses, and preserve all evidence of any kind related to the content, data, software, or accounts associated with such domains, IP addresses, and computer hardware.

IT IS FURTHER ORDERED that Google may serve this Order upon such persons as Google determines are necessary to address and enjoin activity associated with domains and IP addresses identified by Google as being used in connection with the Enterprise, its activities and its botnet, without seeking further leave of the court.

Security for Preliminary Injunction Order

IT IS FURTHER ORDERED that Google's $75,000 bond submitted to the Clerk be returned to Google.

So ordered.

DENISE LOUISE COTE
United States District Judge